AF/2132 IFW
F

OIPE JCWS
JUL 08 2004
PATENT & TRADEMARK OFFICE

Attorney Docket No. 8194-364 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: David R. Irvin
Serial No.: 09/464,363
Filed: December 15, 1999

Confirmation No. 7440
Group Art Unit: 2132
Examiner: Abdulhakim Nobahar

For: **METHODS AND APPARATUS FOR SELECTIVE ENCRYPTION AND DECRYPTION OF POINT TO MULTI-POINT MESSAGES**

Date: July 6, 2004

Mail Stop Appeal Brief-Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

**TRANSMITTAL OF APPEAL BRIEF**
**(PATENT APPLICATION--37 C.F.R. § 1.192)**

1. Transmitted herewith, in triplicate, is the APPEAL BRIEF for the above-identified application, pursuant to the Notice of Appeal filed on June 3, 2004.

2. This application is filed on behalf of
   □ a small entity.

3. Pursuant to 37 C.F.R. § 1.17(c), the fee for filing the Appeal Brief is:

|  |  |  |
|---|---|---|
| □ | small entity | $165.00 |
| ☒ | other than small entity | $330.00 |

Appeal Brief fee due $_330.00______

☒ Any additional fee or refund may be charged to Deposit Account 50-0220.

07/13/2004 HALI11 00000016 09464363
01 FC:1402 330.00 OP

Respectfully submitted,

Robert W. Glatz
Registration No. 36,811

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 20792

**Certificate of Mailing under 37 CFR 1.8 (or 1.10)**
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 6, 2004.

Carey Gregory

O I P E JC67
JUL 0 8 2004
PATENT & TRADEMARK OFFICE

Attorney Docket No. 8194-364 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re: David R. Irvin
Serial No.: 09/464,363
Filed: December 15, 1999
For: **METHODS AND APPARATUS FOR SELECTIVE ENCRYPTION AND DECRYPTION OF POINT TO MULTI-POINT MESSAGES**

Confirmation No. 7440
Group Art Unit: 2132
Examiner: Abdulhakim Nobahar

Date: July 6, 2004

Mail Stop Appeal-Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## APPELLANTS' BRIEF ON APPEAL UNDER 37 C.F.R. §1.192

Sir:

This Appeal Brief is filed pursuant to the "Notice of Appeal to the Board of Patent Appeals and Interferences" filed June 3, 2004.

### Real Party In Interest

Ericsson Inc., a Delaware corporation having a principal place of business at Research Triangle Park, North Carolina.

### Related Appeals

Appellant is aware of no appeals or interferences that would be affected by the present appeal.

### Status of Claims

Appellant appeals the final rejection of Claims 1-8, 10-15 and 24-36, which, as of the filing date of this Brief, remain under consideration. Claims 17-23 and 38-44 have been allowed. Claims 9, 16 and 37 are objected to as dependent on a rejected base claim. The attached Appendix A presents the claims at issue as they currently stand as of the Final Office Action of April 20, 2004 ("Final Action").

### State of Amendments

The attached Appendix A presents the claims as presented in the original application. There have been no amendments to the claims.

## Summary of the Invention

Wireless communications systems are commonly employed to provide voice and data communications to subscribers. Communications in a wireless communications system such as the systems of **FIGs. 1** and **2** of the present application typically make use of different addressing modes for messages sent out by base stations over a broadcast control channel. Messages may be sent to a broadcast address of the communications system, *i.e.* addressed to all the mobile terminals (receiver devices or receivers) served by the system, or sent to an individual address associated with a specific mobile terminal. One problem with such prior art systems is that all mobile terminals having the proper broadcast address may access all messages broadcast with the broadcast address. Thus, it is problematic to conveniently use the same channel to send both messages that are intended to be received generally and those that are intended to be received by only a subset of the potential receivers. This is particularly problematic with the expansion of services available on such communications networks, including the introduction of premium services such as, for example, stock quotes or weather updates. *See* Specification, page 3, line 10-page 3, line 31.

The present invention provides methods and systems for selectively encrypting and decrypting messages transmitted on a broadcast channel of a communication network. Group encryption keys are provided for one or more services utilizing the broadcast channel to communicate messages. A message associated with a particular service first receives an error check value, such as a cyclical redundancy check (CRC) value, generated from the unencrypted message. The message is then encrypted using the group encryption key for the service and the CRC is added to the encrypted message and transmitted with a broadcast address of the communication network. A receiver then receives the message and determines that the CRC indicates an error (as it is generated from the encrypted message rather than the unencrypted message). The receiver then decrypts the message using the group encryption key for the service (assuming the receiver is authorized to receive the service, *i.e.*, has access to the group encryption key) and generates a CRC from the decrypted message. If this CRC matches the CRC received with the message, the receiver recognizes the message as being associated with the corresponding service and processes the message accordingly. Where multiple services are supported and the receiver has a corresponding plurality of group encryption keys, each encryption key can be tested until a CRC without error is provided thereby indicating the service with which the message is associated. *See* Specification, page 4, line 15-page 5, line 2.

In a further aspect of the present invention, a selective encryption system is provided including an encryption circuit that encrypts a message using a group encryption key and an error check value generation circuit that generates an error check value based on the unencrypted message and adds the error check value to the encrypted message. A transmitter broadcasts the encrypted message with the added error check value on a broadcast channel of a communication network and an encryption key selection circuit selects one of a plurality of candidate group encryption keys as the group encryption key based on a service associated with the message. In one embodiment, a receiver is provided that requests the group encryption key and the transmitter is configured to transmit the group encryption key with an individual address of a requesting device responsive to receiving a request for the group encryption key. *See* Specification, page 7, line 29-page 8, line 6.

In another aspect of the present invention, a selective decryption system is provided including a receiver that receives a message on a broadcast channel of a communication network and a decryption circuit that decrypts the message using a group encryption key. An error check value generation circuit generates an error check value for the received message and the decrypted message. A comparator circuit responsive to the error check value generation circuit determines whether an error is indicated for the received message and the decrypted message and a selection circuit responsive to the comparator circuit selects one of the received message or the decrypted message as a message to process. *See* Specification, page 8, lines 7-15.

## **Issues**

1. Are Claims 1-8, 10-13 and 24-34 properly rejected under 35 U.S.C. § 102(e) as being anticipated by United States Patent No. 6,028,860 to Laubach *et al.* (hereinafter "Laubach")?

2. Are Claims 14, 15, 35 and 36 properly rejected under 35 U.S.C. § 103(a) as being unpatentable over Laubach in view of United States Patent No. 6,130,623 to MacLellan *et al.* (hereinafter "MacLellan")?

## Grouping of Claims

For appeal, the claims may be grouped together as follows:

Group I: Claims 1-8, 10-15, 24, 25 and 28-36.

Group II: Claims 26 and 27.

Claims of Groups I do not all stand or fall together as Appellants submit that Claims 10-12 are separately patentable.

## Argument

### I. Introduction

Claims 1-8, 10-13 and 24-34 (all in Group I) of the present application stand rejected under 35 U.S.C. § 102(e) as being anticipated by Laubach. A determination of anticipation under § 102 requires that each and every element of the claim is found in a single prior art reference. *W. L. Gore & Associates Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983). Stated another way, all material elements of a claim must be found in one prior art source. *See In re Marshall*, 198 U.S.P.Q. 344 (C.C.P.A 1978). "Anticipation under 35 U.S.C. § 102 requires the disclosure in a single piece of prior art of each and every limitation of a claimed invention." *Apple Computer Inc. v. Articulate Sys. Inc.*, 57 U.S.P.Q.2d 1057, 1061 (Fed. Cir. 2000). A finding of anticipation further requires that there must be no difference between the claimed invention and the disclosure of the cited reference as viewed by one of ordinary skill in the art. *See Scripps Clinic & Research Foundation v. Genentech Inc.*, 927 F.2d 1565, 1576, 18 U.S.P.Q.2d 1001, 1010 (Fed. Cir. 1991). The Court of Appeals for the Federal Circuit has held that a finding of anticipation requires absolute identity for each and every element set forth in the claimed invention. *See Trintec Indus. Inc. v. Top-U.S.A. Corp.*, 63 U.S.P.Q.2d 1597 (Fed. Cir. 2002). Additionally, the cited prior art reference must be enabling, thereby placing the allegedly disclosed matter in the possession of the public. *In re Brown*, 329 F.2d 1006, 1011, 141 U.S.P.Q. 245, 249 (C.C.P.A. 1964). Thus, the prior art reference must adequately describe the claimed invention so that a person of ordinary skill in the art could make and use the invention. Appellant submits that the Group I claims are not anticipated by Laubach for at least the reason that Laubach fails to disclose or suggest recitations in the independent claims, including the use of encryption in connection with communication of messages as recited therein.

Claims 14, 15, 35 and 36 (all in Group I) of the present application stand rejected as obvious under 35 U.S.C. § 103(a). A determination under §103 that an invention would have been obvious to someone of ordinary skill in the art is a conclusion of law based on fact. *Panduit Corp. v. Dennison Mfg. Co.*, 810 F.2d 1593, 1 U.S.P.Q.2d 1593 (Fed. Cir. 1987), *cert. denied*, 107 S.Ct. 2187. After the involved facts are determined, the decision maker must then make the legal determination of whether the claimed invention as a whole would have been obvious to a person having ordinary skill in the art at the time the invention was made. *See Panduit*, 810 F.2d at 1596. The United States Patent and Trademark Office (USPTO) has the initial burden under § 103 to establish a *prima facie* case of obviousness. *In re Fine*, 837 F.2d 1071, 5 U.S.P.Q.2d 1596, 1598 (Fed. Cir. 1988).

To establish a *prima facie* case of obviousness, the prior art reference or references when combined must teach or suggest **all** the recitations of the claims, and there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. *See* M.P.E.P. § 2143. The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See* M.P.E.P. § 2143.01 (citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990)). As emphasized by the Court of Appeals for the Federal Circuit, to support combining references, evidence of a suggestion, teaching, or motivation to combine must be **clear and particular**, and this requirement for clear and particular evidence is not met by broad and conclusory statements about the teachings of references. *In re Dembiczak*, 50 U.S.P.Q.2d 1614, 1617 (Fed. Cir. 1999). In another decision, the Court of Appeals for the Federal Circuit has stated that, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000).

Furthermore, as stated by the Federal Circuit with regard to the selection and combination of references:

> This factual question of motivation is material to patentability, and could not be resolved on subjective belief and unknown authority. It is improper, in determining whether a person of ordinary skill would have been led to this combination of references, simply to "[use] that which the inventor taught against its teacher." W.L. Gore v. Garlock, Inc., 721 F.2d 1540, 1553, 220 USPQ 303, 312-13 (Fed. Cir. 1983). Thus the Board must not only assure that the requisite findings are made, based on evidence of record, but must also explain the reasoning by which the findings are deemed to support the agency's conclusion....

*In re Sang Su Lee*, 277 F.3d 1338, 1343 (Fed. Cir. 2002).

Appellant submits that the Group I claims and the Group II claims are patentable over the cited references at least because the cited combination fails to disclose or suggest all the recitations of the those claims. The patentability of the currently rejected pending claims is discussed in detail hereinafter.

## II. The Claims Are Not Anticipated by the Cited Prior Art

### A. The Group I Claims Are Not Anticipated by Laubach

The Group I claims stand rejected under § 102(e) as anticipated by Laubach. Appellant submits that Laubach does not disclose or suggest all of the recitations of the Group I claims. Independent Claim 1 recites:

> A method of selective encryption of transmitted messages, comprising the steps of:
> determining a group encryption key for an unencrypted message;
> generating an error check value for the unencrypted message;
> encrypting the unencrypted message using the group encryption key; and
> transmitting the encrypted message and the error check value on a channel of a communication network with an associated destination address. (emphasis added)

Claims 2-8 and 10-15 all depend from Claim 1. Corresponding recitations are found in Claims 24 and 28. Claim 25 depends from Claim 24 and Claims 29-36 depend from Claim 28, and, therefore, the recitations discussed below with respect to Claim 1 are found in all the Group I claims.

Claim 1 recites generating an error check value based on the unencrypted message and transmitting this unencrypted error check value with the encrypted message. The Final Action asserts, with reference to independent Claim 1, that the "header error check (HEC)" of Laubach teaches the "error check value" of Claim 1: "a HEC (or cyclical redundancy check, CRC) is generated for each individual unencrypted message (ATM cell) by a forward error correction processor." Final Action, p. 4. As an initial matter, Appellant notes that there is some confusion as to whether the rejections are based on the HEC of Laubach or the CRC for forward error correction (FEC) of Laubach. Therefore, each aspect of Laubach will be addressed below.

Laubach, unlike the present invention, relates to conventional multi-cast addressing of messages where stations are "assigned one or more station multicast addresses." Laubach, Col. 4, lines 6-7. Laubach describes a virtual connection protocol to "identify one or more subscriber terminal units (STUs) which are to receive the particular cell" based on "virtual path identifiers." Laubach, Col. 7, lines 23-32; Col. 8, lines 29-31. Thus, the distribution of multi-cast communications in Laubach is based on an addressing protocol, not based on the encryption discussed in the present application. *See* Laubach, Col. 10, lines 39-44.

The ATM data of Laubach "refers to cells having a fixed length comprised of a header followed by a payload." Laubach, Col. 6, lines 30-31; Figures 11-12. The HEC is for the unencrypted header of the ATM cell, not the encrypted payload. Laubach, Col. 8, lines 55-61. It is clear from the receive side description in Laubach as well that only the payload, not the header, is encrypted. Laubach, Col. 9, lines 42-50. Thus, if Laubach were to be analogized to Claim 1 of the present application, the payload would correspond to the message that is encrypted. However, such an analogy fails because, as noted above, the HEC of Laubach is based on the header of the ATM cell, not on the payload. Therefore, the HEC of Laubach is not based on the payload so it is irrelevant on whether the payload is encrypted or unencrypted at the time the HEC is calculated. Accordingly, to the extent the rejection is based on the HEC of Laubach, the rejections of the Group I claims should be reversed for at least these reasons.

In response to arguments similar to those offered above, the Final Office Action at page 2 asserts that:

> Laubach on column 8, lines 55-61, describes that the packet data (i.e. the ATM cells) are processed at the ATM cell processor which performs a Header Error Check (HEC) after they are received at the ATM network interface. The ATM cells afterward are sent for encryption to a key handler. The HEC, which is a CRC, is calculated before the encryption of the packet data as also illustrated on Fig. 4 (HEC is computed in block 404 and encryption is performed in block 406), therefore is for the unencrypted packet data (or message). Laubach also on column 8, lines 61, describes that the encryption key is selected from a table with regard to virtual path identifier (VPI) and encryption index. Thus, distribution

> of the encrypted data is dependent on both the VPI (destination address) and the encryption key.

In response, Appellant points out that the Examiner's comments continue to indicate a focus on the encrypted or unencrypted status of the payload when the HEC of Laubach is generated. As noted above, the HEC of Laubach is based on the header, not the payload, of an ATM cell. It is the payload of Laubach that is analogous to the message of the Group I claims. Thus, the response to arguments section of the Final Action again fails to consider the entirety of the claim in applying Laubach against the present application.

With respect to the forward error correction discussion of Laubach, the described CRC for forward error correction is based on the unencrypted header and the encrypted payload. Laubach, Col. 8, lines 60-66; Figure 4. Thus, the CRC (or FEC) is based on the encrypted payload, not the unencrypted payload. The CRC for FEC of Laubach, therefore, is not an error check value for the **unencrypted message** as recited in Claim 1. Therefore, Appellant submits that at least these recitations of the Group I Claims are neither disclosed nor suggested by the CRC for FEC of Laubach.

Additionally, Appellant notes the apparent confusion with regard to the relation of Claims 9-12. The Final Action at page 8 states that Claim 9 "would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims." Thus, Claim 9 recites subject matter already acknowledged as patentable. Claims 10-12 depend from Claim 9 and, therefore, incorporate its subject matter. Appellant submits that Claims 10-12 are separately patentable for at least these reasons.

For at least the reasons described hereinabove, Appellant submits that the Group I Claims are not anticipated by Laubach or obvious over Laubach in combination with MacLellan, which secondary reference addresses none of the shortcomings of Laubach discussed above. Accordingly, Appellant requests that the rejections of the Group I Claims be reversed for at least these reasons.

### B. The Group II Claims Are Not Anticipated by Laubach

The Group II Claims stand rejected as anticipated by Laubach. Independent Claim 26 recites:

> A selective decryption system comprising:
> a receiver that receives a message on a channel of a communication network;
> a decryption circuit that decrypts the message using a group encryption key;

an error check value generation circuit that generates an error check value for the received message and the decrypted message;

a comparator circuit responsive to the error check value generation circuit that determines whether an error is indicated for the received message and the decrypted message; and

a selection circuit responsive to the comparator circuit that selects one of the received message or the decrypted message as a message to process.

Claim 27, the other claim in Group II, depends from Claim 26. The Group II Claims are generally directed to decryption/reception aspects of the present invention, while the Group I Claims are generally directed to encryption/transmission aspects. The distinction between the teachings of Laubach and the Group I Claims is similar to the difference between Laubach and the Group II claims. Claim 26 recites "an error check value generation circuit that generates an error check value for the received message and the decrypted message." This recitation requires that the message is decrypted before the error check value is generated. Accordingly, the rejections of the Group II claims should be reversed for substantially the same reasons as discussed above with reference to the Group I claims.

Appellant notes that the Final Action at page 3 found these arguments persuasive with respect to independent Claims 17 and 38. Those claims are the other independent claims that are directed to the decryption/reception aspects of the present invention. Therefore, Appellant respectfully submits that the rejections of the Group II claims should also be reversed for at least this additional reason.

## III. Conclusion

In light of the above discussion, Appellant submits that each of the pending claims is patentable over the cited references and, therefore, requests reversal of the rejections of Claims 1-8, 10-15 and 24-36 and withdrawal of the objections to Claims 9, 16 and 37.

Respectfully submitted,

Robert W. Glatz
Registration No. 36,811

Myers Bigel Sibley & Sajovec, P.A.
P. O. Box 37428
Raleigh, North Carolina 27627
Telephone: (919) 854-1400
Facsimile: (919) 854-1401
Customer No. 20792

**Certificate of Mailing under 37 CFR 1.8**

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on July 6, 2004.

Carey Gregory

**APPENDIX A**
**Pending Claims USSN 09/464,363**
**Filed December 15, 1999**

1. (original) A method of selective encryption of transmitted messages, comprising the steps of:

determining a group encryption key for an unencrypted message;

generating an error check value for the unencrypted message;

encrypting the unencrypted message using the group encryption key; and

transmitting the encrypted message and the error check value on a channel of a communication network with an associated destination address.

2. (original) A method according to Claim 1, wherein the associated destination address is a broadcast address of the communication network and wherein the channel is a broadcast channel of the communication network.

3. (original) A method according to Claim 2 wherein the step of determining a group encryption key for a message comprises the step of determining a service associated with the message and selecting a group encryption key associated with the determined service.

4. (original) A method according to Claim 2 wherein the step of generating an error check value comprises the step of computing redundancy bits for the message.

5. (original) A method according to Claim 4 wherein the step of transmitting further comprises transmitting the encrypted message with the unencrypted redundancy bits appended to the encrypted message.

6. (original) A method according to Claim 4 wherein the step of determining a group encryption key is preceded by the step of determining if the unencrypted message is intended for a broadcast group having an associated group encryption key; and

wherein the steps of determining a group encryption key, generating an error check value, encrypting the unencrypted message and transmitting the encrypted message are not performed if the unencrypted message is not intended for a broadcast group having an associated group encryption key.

7. (original) A method according to Claim 6 further comprising the steps of:

determining if the unencrypted message is associated with at least one of general broadcast or an individual address;

transmitting the unencrypted message on the broadcast channel of the communication network with the broadcast address of the communication network if the unencrypted message is associated with general broadcast; and

transmitting the unencrypted message on the communication network with the individual address if the unencrypted message is associated with an individual address.

8. (original) A method according to Claim 6 further comprising the steps of:

determining if the unencrypted message is associated with at least one of general broadcast or an individual address;

encrypting the unencrypted message using a general encryption key if the unencrypted message is associated with at least one of general broadcast or an individual address;

generating an error check value based on the encrypted message if the unencrypted message is associated with at least one of general broadcast or an individual address; and

transmitting the encrypted message and the error check value based on the encrypted message on the communication network with the individual address if the unencrypted message is associated with an individual address and with the broadcast address of the communication network if the unencrypted message is associated with general broadcast.

9. (original) A method according to Claim 2 further comprising the steps of:

receiving the encrypted message and added error check value on the broadcast channel of the communication network;

determining if the received message is directed to the broadcast address of the communication network;

generating an error check value for the received message;

determining if the error check value indicates an error;

decrypting the received message using the group encryption key if the received message is directed to a broadcast address of the communication network and the error check value indicates an error;

generating an error check value for the decrypted message; and

assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

10. (original) A method according to Claim 9 wherein the step of determining a group encryption key for an unencrypted message comprises the step of determining one of a plurality of services which is associated with the message and selecting a one of a plurality of group encryption keys which is associated with the determined one of the plurality of services which is associated with the message as the group encryption key for the unencrypted message.

11. (original) A method according to Claim 10 further comprising the step of repeating the steps of decrypting, generating an error check value for the decrypted message and assigning the received message to a group using selected ones of the plurality of group encryption keys as the group encryption key until at least one of the error check value for the decrypted message indicates no error and each of the selected ones of the plurality of group encryption keys has been used as the group encryption key.

12. (original) A method according to Claim 11 further comprising the steps of:

receiving a request for one of the plurality of group encryption keys from a user;

associating the user with a service associated with the requested one of the plurality of group encryption keys; and

transmitting the requested one of the plurality of group encryption keys to the user on the broadcast channel of the communication network with an associated individual address of the user.

13. (original) A method according to Claim 3 further comprising the steps of:

receiving a request for the group encryption key from a user;

associating the user with the service associated with the group encryption key; and

transmitting the group encryption key to the user on the broadcast channel of the communication network with an associated individual address of the user.

14. (original) A method according to Claim 13 wherein the group encryption key has an associated duration and wherein the step of determining a group encryption key for the unencrypted message further comprises the step of updating a group encryption key for the unencrypted message when a previous group encryption key has exceeded its associated duration.

15. (original) A method according to Claim 13 wherein the step of transmitting the group encryption key is followed by the steps of:

updating the group encryption key; and

transmitting the updated group encryption key to users associated with the service associated with the group encryption key using associated individual addresses of the users associated with the service associated with the group encryption key.

16. (original) A method according to Claim 13 further comprising the steps of:

receiving the transmitted group encryption key;

receiving the encrypted message and added error check value on the broadcast channel of the communication network;

determining if the received message is directed to the broadcast address of the communication network;

generating an error check value for the received message;

determining if the error check value indicates an error;

decrypting the received message using the group encryption key if the received message is directed to a broadcast address of the communication network and the error check value indicates an error;

generating an error check value for the decrypted message; and assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

17. (original) A method of selective decryption of transmitted messages, comprising the steps of:

receiving a message on a channel of a communication network;

determining if the received message is directed to a broadcast address of the communication network;

generating an error check value for the received message;

determining if the error check value indicates an error;

decrypting the received message using a group encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates an error;

generating an error check value for the decrypted message; and

assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

18. (original) A method according to Claim 17 wherein the step of decrypting the received message is preceded by the steps of:

transmitting a request for the group encryption key; and

receiving the group encryption key on the channel of the communication network.

19. (original) A method according to Claim 17 further comprising the step of repeating the steps of decrypting, generating an error check value for the decrypted message and assigning the received message to a group using ones of a plurality of group encryption keys as the group encryption key until at least one of the error check value for the decrypted message indicates no error and each of the ones of the plurality of group encryption keys has been used as the group encryption key.

20. (original) A method according to Claim 17 wherein the step of generating an error check value for the decrypted message comprises the steps of:

computing redundancy bits for the decrypted message; and comparing the computed redundancy bits to redundancy bits included with the received message to determine if an error is indicated for the decrypted message.

21. (original) A method according to Claim 17 wherein the step of generating an error check value for the decrypted message comprises the steps of:

applying an error correction code to the decrypted message; and

determining that an error is indicated for the decrypted message if any errors remain in the decrypted message after applying the error correction code to the decrypted message.

22. (original) A method according to Claim 17 further comprising the steps of:

determining if the received message is directed to an individual address of a receiver device receiving the message; and

decrypting the received message using a general encryption key different from the group encryption key if the received message is directed to the individual address.

23. (original) A method according to Claim 22 further comprising the step of decrypting the received message using the general encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates no error.

24. (original) A selective encryption system comprising:

an encryption circuit that encrypts a message using a group encryption key;

an error check value generation circuit that generates an error check value based on the unencrypted message and adds the error check value to the encrypted message;

a transmitter that transmits the encrypted message with the added error check value on a channel of a communication network; and

an encryption key selection circuit that selects one of a plurality of candidate group encryption keys as the group encryption key based on a service associated with the message.

25. (original) A system according to Claim 24 further comprising:

a receiver that receives requests for the group encryption key; and wherein the transmitter is configured to transmit the group encryption key with an individual address of a requesting device responsive to receiving a request for the group encryption key; and

wherein the transmitter transmits the encrypted message with a broadcast address of the communication network.

26. (original) A selective decryption system comprising:

a receiver that receives a message on a channel of a communication network;

a decryption circuit that decrypts the message using a group encryption key;

an error check value generation circuit that generates an error check value for the received message and the decrypted message;

a comparator circuit responsive to the error check value generation circuit that determines whether an error is indicated for the received message and the decrypted message; and

a selection circuit responsive to the comparator circuit that selects one of the received message or the decrypted message as a message to process.

27. (original) A system according to Claim 26 further comprising:

a transmitter that transmits a request for the group encryption key; and

wherein the receiver is configured to receive the group encryption key.

28. (original) A system for selective encryption of transmitted messages, comprising:

means for determining a group encryption key for an unencrypted message;

means for generating an error check value for the unencrypted message;

means for encrypting the unencrypted message using the group encryption key;

means for adding the error check value to the encrypted message; and

means for transmitting the encrypted message and added error check value on a channel of a communication network with an associated destination address.

29. (original) A system according to Claim 28, wherein the associated destination address is a broadcast address of the communication network and wherein the channel is a broadcast channel of the communication network.

30. (original) A system according to Claim 29 wherein the means for determining a group encryption key for a message comprises means for determining a service associated with the message and selecting a group encryption key associated with the determined service.

31. (original) A system according to Claim 29 wherein the means for generating an error check value comprises means for computing redundancy bits for the message.

32. (original) A system according to Claim 31 further comprising:

means for determining if the unencrypted message is associated with at least one of general broadcast or an individual address;

means for transmitting the unencrypted message on a broadcast channel of a communication network with the broadcast address of the communication network if the unencrypted message is associated with general broadcast; and

means for transmitting the unencrypted message on a broadcast channel of a communication network with the individual address if the unencrypted message is associated with an individual address.

33. (original) A system according to Claim 31 further comprising:

means for determining if the unencrypted message is associated with at least one of general broadcast or an individual address;

means for encrypting the unencrypted message using a general encryption key if the unencrypted message is associated with at least one of general broadcast or an individual address;

means for generating an error check value based on the encrypted message if the unencrypted message is associated with at least one of general broadcast or an individual address; and means for adding the error check value based on the encrypted message to the encrypted message if the unencrypted message is associated with at least one of general broadcast or an individual address; and

means for transmitting the encrypted message and the appended error check value based on the encrypted message on a broadcast channel of a communication network with the individual address if the unencrypted message is associated with an individual address and with the broadcast address of the communication network if the unencrypted message is associated with general broadcast.

34. (original) A system according to Claim 30 further comprising:

means for receiving a request for the group encryption key from a user;

means for associating the user with the service associated with the group encryption key; and

means for transmitting the group encryption key to the user on the broadcast channel of the communication network with an associated individual address of the user.

35. (original) A system according to Claim 34 wherein the group encryption key has an associated duration and wherein the means for determining a group encryption key for the unencrypted message further comprises means for updating a group encryption key for the unencrypted message when a previous group encryption key has exceeded its associated duration.

36. (original) A system according to Claim 34 further comprising:

means for updating the group encryption key; and

means for transmitting the updated group encryption key to users associated with the service associated with the group encryption key using associated individual addresses of the users associated with the service associated with the group encryption key.

37. (original) A system according to Claim 34 further comprising:

means for receiving the transmitted group encryption key;

means for receiving the encrypted message and added error check value on the broadcast channel of the communication network;

means for determining if the received message is directed to the broadcast address of the communication network;

means for generating an error check value for the received message;

means for determining if the error check value indicates an error;

means for decrypting the received message using the group encryption key if the received message is directed to a broadcast address of the communication network and the error check value indicates an error;

means for generating an error check value for the decrypted message; and

means for assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

38. (original) A system for selective decryption of transmitted messages, comprising:

means for receiving a message on a channel of a communication network;

means for determining if the received message is directed to a broadcast address of the communication network;

means for generating an error check value for the received message;

means for determining if the error check value indicates an error;

means for decrypting the received message using a group encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates an error;

means for generating an error check value for the decrypted message; and

means for assigning the received message to a group associated with the group encryption key if the error check value for the decrypted message indicates no error.

39. (original) A system according to Claim 38 further comprising:

means for transmitting a request for the group encryption key; and

means for receiving the group encryption key on the channel of the communication network.

40. (original) A system according to Claim 38 further comprising means for repeating the steps of decrypting, generating an error check value for the decrypted message

and assigning the received message to a group using ones of a plurality of group encryption keys as the group encryption key until at least one of the error check value for the decrypted message indicates no error and each of the ones of the plurality of group encryption keys has been used as the group encryption key.

41. (original) A system according to Claim 38 wherein the means for generating an error check value for the decrypted message further comprises:

means for computing redundancy bits for the decrypted message; and

means for comparing the computed redundancy bits to redundancy bits included with the received message to determine if an error is indicated for the decrypted message.

42. (original) A system according to Claim 38 wherein the means for generating an error check value for the decrypted message further comprises:

means for applying an error correction code to the decrypted message; and

means for determining that an error is indicated for the decrypted message if any errors remain in the decrypted message after applying the error correction code to the decrypted message.

43. (original) A system according to Claim 38 further comprising:

means for determining if the received message is directed to an individual address of a receiver device receiving the message; and

means for decrypting the received message using a general encryption key different from the group encryption key if the received message is directed to the individual address.

44. (original) A system according to Claim 43 further comprising means for decrypting the received massage using the general encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates no error.